

REMARKS

Please reconsider the claims in the application in view of the remarks below.

Claim Rejection – 35 U.S.C. §103(a)

The Office Action rejected claims 1, 2, 12-15, 25, 26 and 33 under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 6,405,315 (“Burns”) in view of U.S. Patent No. 6,959,384 (“Serret-Avila”). The Office Action rejected claims 3, 7-8, 10, 11, 20, 21, 23, 27, 29-32 under 35 U.S.C. §103(a) as allegedly being unpatentable over Burns in view of Serret-Avila and further in view of U.S. Patent No. 6,931,543 (“Pang”), in view of U.S. Patent No 5,124,117 (“Tatebayashi”). Claims 4, 17 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Burns and Serret-Avila in view of U.S. Patent No. 5,608,801 (“Aiello”). Of the pending claims, claims 1, 14, 25 and 33 are independent.

The Office Action maintained the same previous rejections of the claims. In responding to the applicants’ previous arguments that Burns and Serret-Avila do not disclose or suggest storing integrity tree data structure at the client, the Examiner further responds that, “Burns does in face disclose that when a client requests access to the stored data, the data is sent to the network client, decrypted, hashed and verified by comparing the calculated hash with the previously calculated hashed that was stored with the data,” citing Burns, Col. 8, lines 5-10 & Col. 10, line 60 – Col. 11, line 17. The Examiner misinterprets those passages of Burns. As understood by applicants, Burns in Col. 8, lines 5-10 describes file system structure, specifically directory data object stored on a network storage device, not at the client. That passage of Burns appears to describe that its directory data object stored on a network storage device includes

chunks of data and hash of the data. Reading of Burns, Col. 7, lines 50-51 supports this understanding. Thus, Burns in Col. 8, lines 5-10 does not disclose or suggest that hash is stored with its client. Rather, Burns stores the hash of data with the data at the network storage device. Further, Col 10, line 60 – Col. 11, line 17 of Burns, as understood by applicants, discloses reading that stored data and hash of the data from the storage device, and comparing with a calculated hash. Thus, Burns does not disclose or suggest storing hash at the client. Serret-Avila also does not make up for that deficiency.

In the present application, the root of the integrity tree is stored on the client (“customer”) computer that uses the storage utility. An integrity check of data retrieved from the network storage utility is performed by using the “stored integrity value” stored on the client.

While the above reasons suffice to overcome the rejections of independent claims 1, 14, 25 and 33, applicants in this reply are amending the claims to recite, “on the client device when said one or more data blocks are written out to the network-attached storage device,” in order to further clarify what is being claimed. Support for the amendment can be found at least in paragraphs [0014] and [0016].

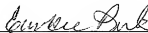
For at least the above reason, applicants believe that independent claims 1, 14, 25 and 33, and their respective dependent claims at least by virtue of their dependency are not obvious over Burns and Serret-Avila.

With respect to the dependent claims rejected also in view of the rest of the references, because those references fail to disclose or suggest what Burns and Serret-Avila lack as explained above with respect to independent claims, those dependent claims also are believed to be unobvious over the cited references.

In addition, with specific reference to the rejection of claim 11, the Examiner errs in alleging Burns in Col. 5, lines 40-45 discloses, "comparing integrity of data blocks to be read on a path from said root data structure via successive higher meta-data blocks and meta-data block layers until a desired data block at a first layer is read." That passage of Burns refers to a client wanting to update a network object reads the data, decrypts, updates and encrypts the data. Burns, however, does not disclose or suggest comparing the integrity of data blocks to be read on a path from said root data structure via successive layers.

In view of the foregoing, this application is now believed to be in condition for allowance, and a Notice of Allowance is respectfully requested. If the Examiner believes a telephone conference might expedite prosecution of this case, applicant respectfully requests that the Examiner call applicant's attorney at (516) 742-4343.

Respectfully submitted,


Eunhee Park
Registration No.: 42, 976

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, N.Y. 11530
(516) 742-4343